Measures to minimise internet tracking

September 2020

Introduction

When using The Internet, certain practices affect your privacy - such as browsing activity tracking on many websites. This is usually done through cookies - mainly advertising or analytics cookies. Their aim is to create profiles with a view to offering advertising that aligns with the interests and specific characteristics of each person. They are also used for collecting statistical information about accessing online services.

When you visit a website, you are not just accessing one single webpage. You are also redirected in parallel to multiple third-party servers that generally provide advertising and data analysis services for the main website. Giving these third parties access is what allows them to install and access information linked to the cookies[1] that track the activities of each user. This is why most techniques used to improve user control over internet tracking are based on the option of minimising third-party cookies, or directly preventing access to those third parties.

Although it is the best-known method, it is not just cookies that are used to track someone as they browse online. Other techniques are used to achieve the same purpose, including those based on unique advertising identifiers[2], or those implemented by obtaining the device fingerprint[3]. In browsers, Local Storage and IndexedDB also allow information on the device to be stored and retrieved while browsing, and can also be used for tracking user activity. Server logs (which record activity) can also be exploited in this way by correlating information stored on various sites. Therefore, preventing access to services that do this without offering appropriate guarantees is the most effective method of protecting your privacy.

Please keep in mind that these user-tracking techniques are not unique to browsers on personal computers. Mobile phones, tablets and other smart devices, such as Smart TVs, also use unique advertising identifiers. These identifiers are sent to internet servers when an app is used and when certain events occur, allowing the user to be identified and tracked.

Something else to keep in mind is that web browsers and devices also allow you to log in, for example, with an email account. This allows direct access to email and many other applications directly from the browser interface and options, as well as maintaining options for personalising services. Once the user session is started, the browsing history can be automatically sent to the provider of that service.

It is also possible to track user activity through federated authentication services offered by large internet and social network companies. This happens when you can use your Facebook, Google or other accounts to sign in a particular website or application.

[1] Guide to the use of cookies. AEPD.
[2] Technical note: User control when customising Android advertisements. AEPD.
[3] Device fingerprinting study. AEPD.

Basic recommendations

The following are basic recommendations for users without advanced knowledge to minimise unwanted exposure of personal data:

1. Consider privacy to be a desirable feature when choosing a browser and any applications you install and use on your devices. Due to the way these products are constantly evolving you should check the most recent analyses published about them.

2. Avoid installing unnecessary applications on your browser, as this will minimise risks.

3. Keep your browser up to date with the latest tracking protection technologies.

4. If your browser has advanced tracking protection[4], activate it and keep it on. These options allow for various levels of protection. Choose the highest level to suit your preferences. In any case, you can if you wish enable the option to send a "Do not track"[5] signal to websites.

5. If you wish, you can set your browser to block third-party cookies[6], or at least block them when you browse in private mode. In browsers with anti-tracking/tracking protection, these options will be integrated under the settings.

6. Consider having two different browsers: one with more restrictive setting; the other, configured with higher permissions. This means that if the browser with more restrictive settings prevents you from accessing a particular service, you can use the other browser to access that service, thus minimising the exposure of your data.

7. Another option when browsing sites that require greater access to your data is to add an exception in your browser settings, but remember that you will be exposing personal information with the sites included in the exception.

8. You can set the browser so that cookies are deleted when you close it. If this does not suit you when browsing your favourite sites, you can choose to delete the cookies manually every so often.

9. Prevent to log in to the browser if you can, identifying yourself with a user, or at least, avoid keeping the session open indefinitely. Also, set the browser so that it does not synchronise your browsing data with your session user.

10. If the browser does not have advanced tracking protection, you can install extensions to do this. However, only install extensions that offer guarantees. In general, installing third-party software on top of your browser can introduce risks.

11. You can, if you wish, set your device options so that the advertising identifier is not used to create profiles or display tailored advertisements based on your location or profile. If your device allows, you can also change[7] the advertising identifier every so often under privacy settings.

12. Review and configure customisation, profile and advertising options for any applications, services and social networks[8] you use.

[4] Tracking protection on Mozilla Firefox and Microsoft Edge.
[5] "Do Not Track" signal settings on Chrome, Firefox and Edge.
[6] Third-party cookie blocking on Chrome, Firefox and Edge.
[7] Changing/resetting the advertising identifier in Android and iOS.
[8] Advertisement personalisation control for Twitter, Facebook and Google.

Recommendations for advanced users

Advanced techniques can be used to achieve a higher level of control and protection against unwanted monitoring on The Internet - including:

1. Setting up a DNS query blocker - such as PiHole[9] - on your home network. This allows you to add lists of domains that connections from devices on your network are restricted.

2. Browse via a VPN (virtual private network) or the TOR[10] network. Keep in mind that using these services inappropriately can pose other risks to privacy and security in your connections.

3. Install virtual machines on your system, including just a web browser and browse under virtual sessions.

4. Use operating systems that are designed to preserve privacy and anonymity, such as Tails[11] and QubesOS[12].

[9] https://pi-hole.net/
[10] https://www.torproject.org/es/
[11] https://tails.boum.org/install/
[12] https://www.qubes-os.org/intro/